YOUWEI ZHONG

Shanghai Jiao Tong University ◇ Shanghai, China
Currently at Yale University ◇ New Haven, US
youwei@ywzh.org ◇ https://ywzh.org/

EDUCATION

Shanghai Jiao Tong University *September 2021 – Present*
Undergraduate in Computer Science
Member of **John Hopcroft Class**, an elite CS program at Zhiyuan College, Shanghai Jiao Tong University, for top 10% of students, with a focus on **Theoretical Computer Science**.

Core GPA: 3.91
Cumulative GPA: 3.88
TOEFL Score: 104

PUBLICATION

A Parameterized Framework for the Formal Verification of Zero-Knowledge Virtual Machines 2024
Youwei Zhong (sole student author) *OOPSLA 2024*

- Advised by Qinxiang Cao and Yuncong Hu
- **The Second Place Winner** in the Student Research Competition

MANUSCRIPTS

A Parameterized Verification Framework for the Constraint Generation Algorithms in Zero-Knowledge Virtual Machines 2025
Youwei Zhong, Zihan Xu, Haixing He, Yuncong Hu, Xiang Xie, Qinxiang Cao *In submission to Asiacrypt'25*

- This paper is an extension work based on my OOPSLA 2024 SRC paper. We formalize the cryptographic security properties of zkVMs in the Coq proof assistant, including soundness, completeness, knowledge soundness, and zero-knowledge, by formalizing probabilistic programs using monads.

RESEARCH EXPERIENCE

Rigorous Software Engineering (ROSE) group, Yale University November 2024 - May 2025
Research internship advised by Ruzica Piskac, Timos Antonopoulos and Ning Luo *New Haven, Connecticut, US*

- Extended the Ou-Lian programming framework, which is used to compile input ZKP protocols into circuits so that it can examine chains of optimizations carefully aligned with the compilation process. (on-going)
- Developed automated tools to validate and synthesize optimized R1CS circuits. (on-going)

Programming Languages and Software Engineering (PLSE) group, University of California Santa Barbara / Riema Labs March 2024 - October 2024
Research internship advised by Yu Feng and Yanju Chen, in collaboration with Ranjit Jhala *Remote*

- Wrote bug detector prototypes by doing regular matching on the MIR of Rust programs used in Scroll zkEVM. Experimented on using LLMs to detect bugs in our benchmark.
- Developed bug finders for zero-knowledge virtual machines by synthesizing stub specifications with abstract interpretation to enable modular verification using the Flux refinement type checker
- Developed an analyzer that translates Circom programs into C programs, which uses the KLEE symbolic execution engine to detect unconstrained zero-knowledge circuits.

John Hopcroft Center, Shanghai Jiao Tong University April 2023 - October 2024
Research internship advised by Qinxiang Cao and Yuncong Hu *Shanghai, China*

- Developed a parameterized framework for the formal verification of zero-knowledge virtual machines, using the Coq proof assistant. Verified the parameterized constraint generation algorithm used by zero-knowledge virtual machines. Instantiated our parameterized framework on two examples: Cairo VM and a simplified zkEVM. (paper accepted by OOPSLA 2024 SRC, extension work in progress)
- Developed a DSL in Coq that provides a built-in field element type. Enabled symbolic execution and entailment generation in our DSL. Wrote an example of proving the correctness of a bit-decomposition program in our DSL.

ACADEMIC ACTIVITIES

OOPSLA/SPLASH 2024 October 2024
Student Volunteer *Pasadena, California, United States*

- Attended the Programming Languages Mentoring Workshop (PLMW).
- Participated in the Student Research Competition and got the 2nd place in undergraduate category.

WORK EXPERIENCE

Minghong Investment January 2024 - February 2024
Quantitative Developer *Shanghai, China*

- Worked in developing a high frequency trading system.
- Updated C++ system interfaces based on the RDB database format.
- Processed data from different cryptocurrency exchanges.

TEACHING EXPERIENCE

CS1207, Programming and data structure - III, Shanghai Jiao Tong University June 2023 – July 2023
Teaching assistant *Shanghai, China*

- Prepared the code repository for the project of Ray Tracing in Rust. Wrote a detailed setup manual for the students.
- Designed the tasks of the project. Answered the questions of the students.

HONORS AND AWARDS

The 2nd Place Winner in OOPSLA 2024 SRC (300 USD) October 2024
Longfor Scholarship (10'000 yuan, 10 winners each year) December 2022
Zhiyuan Honors Scholarship (5'000 yuan per year, Top 10%) December 2023, 2022 and 2021
Three Good Student of Shanghai Jiao Tong University October 2024, 2023 and 2022
A-class Academic Excellence Scholarship December 2024

MISCELLANEOUS

John Class Online December 2021 – Present
Maintainer

- Designed an internal class forum based on Discourse, a well-known open source discussion platform.
- Maintained the operation of the Aliyun server and the website.

Zhiyuan College Debate Team July 2021 – July 2022
Captain *Shanghai, China*

- Organized the recruitment of the debate team. Produced recruiting WeChat pushes.
- Lead the preparation for Freshman Cup and Union Cup. Organized team building activities.

TECHNICAL SKILLS

Research Interests	Formal Verification, Zero-Knowledge Proof
Computer Languages	Coq, C, C++, Python, Rust
Machine Learning library	Pytorch, Scikit-learn
Tools	Git, VSCode